UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

FREDERICK F. WHELAN, JR. DOUGLAS R. EMERICK, and JASON ALBERT, on behalf of themselves individually and on behalf of all others similarly situated, Plaintiffs, v. GERSON LEHRMAN GROUP, INC, Defendant.	**CASE NO. 24-2202** **CLASS ACTION COMPLAINT** **JURY DEMAND**

CLASS ACTION COMPLAINT

Plaintiffs FREDERICK F. WHELAN, JR., DOUGLAS R. EMERICK, and JASON ALBERT ("Plaintiffs") bring this Class Action Complaint ("Complaint") against Defendant GERSON LEHRMAN GROUP, INC ("GLG" or "Defendant") as individuals and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions and their counsels' investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. This Class Action arises from a recent cyberattack resulting in a data breach of sensitive information in the possession and custody and/or control of Defendant (the "Data Breach").

2. The Data Breach resulted in the unauthorized disclosure, exfiltration, and theft of consumers' highly personal information, including names and Social Security numbers, ("personal identifying information" or "PII").

3. GLG Data Breach not only affects current and former employees and job applicants, but also affects consumers who had no direct employment or client relationship with GLG, never sought one, and never consented to GLG collecting and storing their information.

4. On information and belief, the Data Breach occurred on November 12, 2023. However, GLG did not become aware of suspicious activity on its network until February 5, 2024, an appalling eighty-five (85) days after the Data Breach had first begun.

5. On March 12, 2024, GLG finally notified state Attorneys General and many putative Class Members about the widespread Data Breach ("Notice Letter"). Plaintiff Whelan's Notice Letter is attached as **Exhibit A**. A standard Notice Letter is attached as **Exhibit B.** GLG waited over a month after discovering the Data Breach before informing Class Members, even though Plaintiffs and a staggering 152,621 Class Members had their most sensitive personal information accessed, exfiltrated, and stolen, causing them to suffer ascertainable losses in the form of the loss of the benefit of their bargain and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

6. GLG's Breach Notice obfuscated the nature of the breach and the threat it posted—refusing to tell its employees, applicants, and consumers how many people were impacted, how the breach happened on GLG's systems, when the breach first occurred, when GLG discovered the Data Breach, or why it took GLG over a month to begin notifying victims that hackers had gained access to highly sensitive PII.

7. Defendant's failure to timely detect and report the Data Breach made its employees, applicants, and consumers vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their PII.

8. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII misuse.

9. In failing to adequately protect Plaintiffs' and the Class's PII, failing to adequately notify them about the breach, and by obfuscating the nature of the breach, Defendant violated state and federal law and harmed an unknown number of its current and former employees, applicants and consumers.

10. Plaintiffs and members of the proposed Class are victims of Defendant's negligence and inadequate cyber security measures. Specifically, Plaintiffs and members of the proposed Class trusted Defendant with their PII. But Defendant betrayed that trust. Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

11. Plaintiffs are Data Breach victims.

12. Accordingly, Plaintiffs, on their own behalf and on behalf of a class of similarly situated individuals, bring this lawsuit seeking injunctive relief, damages, and restitution, together with costs and reasonable attorneys' fees, the calculation of which will be based on information in Defendant's possession.

PARTIES

13. Plaintiff, Frederick F. Whelan, Jr., is a natural person and citizen of Massachusetts, where he intends to remain.

14. Plaintiff, Douglas R. Emerick, is a natural person and citizen of Pennsylvania, where he intends to remain.

15. Plaintiff, Jason Albert, is a natural person and citizen of Florida, where he intends to remain.

16. Defendant, GLG, is a New York and Delaware corporation, incorporated in Delaware with its principal place of business at 60 E 42nd Street, New York 10165.

JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class. At least one Plaintiff and Defendant are citizens of different states.

18. This Court has personal jurisdiction over Defendant because Defendant maintains its principal place of business in this District and does substantial business in this District.

19. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claim occurred in this District.

STATEMENT OF FACTS

GLG

20. GLG touts itself to be the "world's largest insight network" and works with "thousands of clients, companies, and experts to develop the world's most robust compliance framework for primary research"[1] GLG boasts a total annual revenue of $643 million.[2]

21. GLG's software services are specialized for companies and clients who oversee highly sensitive data. GLG thus must oversee, manage, and protect the PII of its clients' employees and consumers, GLG's consumers.

22. On information and belief, these third-party consumers, whose PII was collected by GLG, do not directly do any business with GLG.

[1]GLG, https://glginsights.com/ (last visited March 20, 2024).
[2] GLG, https://www.zoominfo.com/c/gerson-lehrman-group-inc/30936167 (last visited March 20, 2024).

23. As a self-proclaimed leader in its industry handling highly sensitive aspects of its clients' business, GLG understood the need to protect not only its own employees' and applicants' data, but also the client's employees' and consumers' data, as well as prioritize its data security.

24. Indeed, GLG promises in its privacy policy that it has implemented "appropriate technical and organizational security measures", and that it will take "all reasonable measures to protect your Personal Data[.]"[3]

> We have implemented appropriate technical and organisational security measures designed to protect your Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, unauthorised access, and other unlawful or unauthorised forms of Processing, in accordance with applicable law.

25. Despite recognizing its duty to do so, on information and belief, GLG has not implemented reasonably cybersecurity safeguards or policies to protect its consumers' PII or supervised its IT or data security agents and employees to prevent, detect, and stop breaches of its systems. As a result, GLG leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to consumers' PII.

The Data Breach

26. As a condition of employment with GLG, Defendant requires its applicants, employees, including Plaintiffs Albert and Emerick, to disclose PII including but not limited to, their names and Social Security numbers. Defendant used that PII to facilitate its application of employment of Plaintiffs Albert and Emerick, including payroll, and required Plaintiffs Albert and Emerick to provide that PII to apply for employment and payment for that employment.

[3]Privacy Policy, GLG, https://glginsights.com/privacy-policy/ (last visited March 20, 2024).

27. As a condition of employment with GLG, Defendant requires its independent consultants, including Plaintiff Whelan, to disclose PII, including but not limited to, their names and Social Security numbers. Defendant required Plaintiff Whalen to provide that PII to facilitate payment for his independent consultant services.

28. On information and belief, Defendant collects and maintains current and former employees', independent consultants', applicants', and consumers' PII in its computer systems.

29. In collecting and maintaining PII, Defendant implicitly agrees that it will safeguard the data using reasonable means according to its internal policies, as well as state and federal law.

30. According to the Maine Attorney General Data Breach Notification Page, on February 5, 2024, GLG discovered that it had "experienced a ransomware incident in which an unauthorized third party accessed data from GLG's computer system." Ex. B. Following an internal investigation, GLG discovered that the Data Breach had occurred as early as November 12, 2023.[4]

31. In other words, GLG's investigation revealed that its network had been hacked by cybercriminals an appalling three months before notice and that Defendant's cyber and data security systems were completely inadequate and allowed cybercriminals to obtain files containing a treasure trove of thousands of its employees', independent contractors', applicants', and consumers' highly private PII.

32. Most data breach notice letters will, at minimum, admit to the date of the breach as well as when the breach was discovered. Not Defendant. Instead, Defendant intentionally

[4] Data Breach Information, Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/33265961-07d6-49e1-ab43-fa17ca9da3b0.shtml (last visited March 20, 2024).

obfuscates the appallingly long period between the date of the Breach and when Defendant discovered it, leaving Plaintiffs and Class Members in the dark.

33. Through its inadequate security practices, Defendant exposed Plaintiffs' and the Class's PII for theft and sale on the dark web.

34. On or around March 12, 2024, four months after the Breach first occurred – GLG finally notified Plaintiffs and Class Members about the Data Breach.

35. Despite its duties and alleged commitments to safeguard PII, Defendant did not in fact follow industry standard practices in securing applicants' and consumers' PII, as evidenced by the Data Breach.

36. In response to the Data Breach, Defendant contends that it has or will be "strengthening our systems' security[.]" Ex. A. Although Defendant fails to expand on what these alleged "strengthening" of systems are, such steps should have been in place before the Data Breach.

37. Through its Breach Notice, Defendant also recognized the actual imminent harm and injury that flowed from the Data Breach, so it encouraged breach victims to "vigilant and monitor your accounts for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for suspicious or unusual activity." Ex. B.

38. Through the Data Breach, Defendant recognized its duty to implement reasonable cybersecurity safeguards or policies to protect consumers PII, insisting that, despite the Data Breach demonstrating otherwise, Defendant "[t]he protection and proper use of your information is a top priority for GLG." Ex. A.

39. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiffs' and the Class's PII.

Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiffs' and the Class's financial accounts.

40. On information and belief, GLG has offered several months of complimentary credit monitoring services to victims, which does not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the breach involves PII that cannot be changed, such as Social Security numbers.

41. Even with several months of credit monitoring services, the risk of identity theft and unauthorized use of Plaintiffs' and Class Members' PII is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

42. Because of the Data Breach, Defendant inflicted injuries upon Plaintiffs and Class Members. And yet, Defendant has done absolutely nothing to provide Plaintiffs and the Class Members with relief for the damages they suffered and will suffer.

43. On information and belief, Defendant failed to adequately train and supervise its IT and data security agents and employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over its consumers' PII. Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII.

The Data Breach was a Foreseeable Risk of which Defendant was on Notice.

44. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the industry preceding the date of the breach.

45. In light of recent high profile data breaches at other companies in its industry, Defendant knew or should have known that its electronic records and consumers' PII would be targeted by cybercriminals.

46. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[5] The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[6]

47. Indeed, cyberattacks against the healthcare industry have become increasingly common for over ten years, with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime." [7]

48. Cyberattacks on companies like Defendant have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[8]

---

[5] 2021 Data Breach Annual Report, ITRC, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf (last visited June 5, 2023).
[6] *Id*.
[7] Gordon M. Snow Statement, FBI https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector (last visited March 13, 2023).
[8] Secret Service Warn of Targeted, Law360, https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited March 13, 2023).

49. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including GLG.

Plaintiff Whelan's Experience

50. Plaintiff Whelan received GLG's Breach Notice on or around March 12, 2024.

51. Defendant deprived Plaintiff Whelan of the earliest opportunity to guard himself against the Data Breach's effects by failing to notify him about it for at least a month.

52. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff Whelan's PII for theft by cybercriminals and sale on the dark web.

53. As a result of the Data Breach notice, Plaintiff Whelan spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, self-monitoring him accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

54. Plaintiff Whelan has and will spend considerable time and effort monitoring his accounts to protect himself from additional identity theft. Plaintiff Whelan fears for his personal financial security and uncertainty over what PII was exposed in the Data Breach.

55. Plaintiff Whelan has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

56. Plaintiff Whelan suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PII—a form of intangible property that Plaintiff Whelan entrusted to Defendant, which was compromised in and as a result of the Data Breach.

57. Plaintiff Whelan suffered actual injury from the exposure and theft of his PII—which violates his rights to privacy.

58. Plaintiff Whelan has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized third parties and possibly criminals.

59. Plaintiff Whelan has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Emerick's Experience

60. Plaintiff Emerick received GLG's Breach Notice on or around March 20, 2024.

61. Defendant deprived Plaintiff Emerick of the earliest opportunity to guard himself against the Data Breach's effects by failing to notify him about it for at least a month.

62. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff Emerick's PII for theft by cybercriminals and sale on the dark web.

63. As a result of the Data Breach notice, Plaintiff Emerick spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, self-monitoring him accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

64. Plaintiff Emerick has and will spend considerable time and effort monitoring his accounts to protect himself from additional identity theft. Plaintiff Emerick fears for his personal financial security and uncertainty over what PII was exposed in the Data Breach.

65. Plaintiff Emerick has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

66. Plaintiff Emerick suffered actual injury in the form of damages to and diminution in the value of Plaintiff Emerick's PII —a form of intangible property that Plaintiff Emerick entrusted to Defendant, which was compromised in and as a result of the Data Breach.

67. Plaintiff Emerick suffered actual injury from the exposure and theft of his PII—which violates his rights to privacy.

68. Plaintiff Emerick has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized third parties and possibly criminals.

69. Indeed, following the Data Breach, Plaintiff Emerick has experienced an enormous increase in spam calls, suggesting that his PII has been stolen and is now in the hands of cybercriminals.

70. Once an individual's PII is for sale and access on the dark web, as Plaintiffs' PII is here as a result of the Breach, cybercriminals are able to use the stolen and compromised to gather and steal even more information.[9] On information and belief, Plaintiff Emerick's phone number was compromised as a result of the Data Breach.

[9] What do Hackers do with Stolen Information, Aura, https://www.aura.com/learn/what-do-hackers-do-with-stolen-information (last visited January 9, 2024).

71. Plaintiff Emerick has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Albert's Experience

72. Plaintiff Albert received GLG's Breach Notice on or around March 20, 2024.

73. Defendant deprived Plaintiff Albert of the earliest opportunity to guard himself against the Data Breach's effects by failing to notify him about it for at least a month.

74. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff Albert's PII for theft by cybercriminals and sale on the dark web.

75. As a result of the Data Breach notice, Plaintiff Albert spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, self-monitoring him accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

76. Plaintiff Albert has and will spend considerable time and effort monitoring his accounts to protect himself from additional identity theft. Plaintiff Albert fears for his personal financial security and uncertainty over what PII was exposed in the Data Breach.

77. Plaintiff Albert has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

78. Plaintiff Albert suffered actual injury in the form of damages to and diminution in the value of Plaintiff Albert's PII —a form of intangible property that Plaintiff Albert entrusted to Defendant, which was compromised in and as a result of the Data Breach.

79. Plaintiff Albert suffered actual injury from the exposure and theft of his PII—which violates his rights to privacy.

80. Plaintiff Albert has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized third parties and possibly criminals.

81. Indeed, following the Data Breach on or around January 14, 2024, Plaintiff Albert was notified by his bank, Regions Bank, of an attempted fraudulent transaction of $1,149.00 for an item identified as "Power NBA" that Plaintiff Albert did not recognize. On February 26, 2024, Plaintiff Albert was alerted to a second fraudulent transaction of $20.00, for a website titled "Encore" that Plaintiff Albert again did not recognize. These fraudulent transactions suggest that his PII, including his bank account information, which was provided to Defendant during his employment, has been stolen as a result of the Data Breach and is now in the hands of cybercriminals.

82. Further, once an individual's PII is for sale and access on the dark web, as Plaintiffs' PII is here as a result of the Breach, cybercriminals are able to use the stolen and compromised to gather and steal even more information.[10] On information and belief, Plaintiff Albert's bank account was compromised as a result of the Data Breach.

83. Also following the Data Breach, Plaintiff Albert, who utilizes multi-factor authentication, has received numerous notifications of attempts by unauthorized actors attempting to access the email address he provided to GLG during his employment. These

[10] What do Hackers do with Stolen Information, Aura, https://www.aura.com/learn/what-do-hackers-do-with-stolen-information (last visited January 9, 2024).

unauthorized attempts to access his email account further demonstrate his PII has been stolen as a result of the Data Breach and is now in the hands of cybercriminals.

84. Finally, Plaintiff Albert has experienced an enormous increase in spam calls and emails following the Data Breach. On information and belief, Plaintiff Albert's phone was compromised as a result of the Data Breach, as cybercriminals are able to use an individuals PII that is accessible on the dark web, as Plaintiff Albert's is here, to gather and steal even more information.[11]

85. Plaintiff Albert has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiffs and the Proposed Class Face Significant Risk of Continued Identity Theft

86. Plaintiffs and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendant.

87. As a result of Defendant's failure to prevent the Data Breach, Plaintiffs and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

[11] What do Hackers do with Stolen Information, Aura, https://www.aura.com/learn/what-do-hackers-do-with-stolen-information (last visited January 9, 2024).

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII in its possession.

88. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.

89. The value of Plaintiffs' and the Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen PII openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

90. It can take victims years to spot identity theft, giving criminals plenty of time to use that information for cash.

91. One such example of criminals using PII for profit is the development of "Fullz" packages.

92. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

93. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiffs and the proposed Class' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs' and the Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

94. Defendant disclosed the PII of Plaintiffs and the Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiffs and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

95. Defendant's failure to properly notify Plaintiffs and members of the Class of the Data Breach exacerbated Plaintiffs' and the Class's injury by depriving them of the earliest

ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendant failed to adhere to FTC guidelines.

96. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PII.

97. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the sensitive consumer information that it keeps;

b. properly dispose of PII that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

98. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

99. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

100. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

101. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to its employees' applicants', and consumers' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Fails to Comply with Industry Standards

102. As noted above, experts studying cyber security routinely identify entities in possession of PII as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

103. Several best practices have been identified that a minimum should be implemented by employers in possession of PII, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

104. Other best cybersecurity practices that are standard for employers include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as

firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

105. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

106. These foregoing frameworks are existing and applicable industry standards for an employer's obligations to provide adequate data security for its employees. Upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

CLASS ACTION ALLEGATIONS

107. Plaintiffs bring this class action under Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the following class:

> All individuals residing in the United States whose PII was compromised in the GLG Data Breach including all those who received notice of the breach.

108. Excluded from the Class is Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant have a controlling interest, any of Defendant's officers or directors, any successors, and any Judge who adjudicates this case, including their staff and immediate family.

109. Plaintiffs reserve the right to amend the class definition.

110. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

a. **Numerosity**. Plaintiffs are representative of the Class, consisting of at least 152,621 members, far too many to join in a single action;

b. **Ascertainability**. Members of the Class are readily identifiable from information in Defendant's possession, custody, and control;

c. **Typicality**. Plaintiffs' claims are typical of class claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

d. **Adequacy**. Plaintiffs will fairly and adequately protect the proposed Class's interests. Their interests do not conflict with the Class's interests, and they have retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

e. **Commonality**. Plaintiffs' and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for the Class. Indeed, it will be necessary to answer the following questions:

i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiffs' and the Class's PII;

ii. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

iii. Whether Defendant were negligent in maintaining, protecting, and securing PII;

iv. Whether Defendant breached contract promises to safeguard Plaintiffs' and the Class's PII;

v. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

vi. Whether Defendant's Breach Notice was reasonable;

vii. Whether the Data Breach caused Plaintiffs' and the Class's injuries;

viii. What the proper damages measure is; and

ix. Whether Plaintiffs and the Class are entitled to damages, treble damages, or injunctive relief.

111. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

COUNT I
Negligence
(On Behalf of Plaintiffs and the Class)

112. Plaintiffs reallege all previous paragraphs as if fully set forth below.

113. Plaintiffs and members of the Class entrusted their PII to Defendant. Defendant owed to Plaintiffs and the Class a duty to exercise reasonable care in handling and using the PII in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

114. Defendant owed a duty of care to Plaintiffs and members of the Class because it was foreseeable that Defendant's failure to adequately safeguard their PII in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that PII —just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and the Class's PII by disclosing and providing access to this information to unauthorized third parties and by failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

115. Defendant owed to Plaintiffs and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiffs and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiffs and the Class to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

116. Defendant owed these duties to Plaintiffs and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiffs' and the Class's PII.

117. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable

that unauthorized individuals would attempt to access Defendant's databases containing the PII —whether by malware or otherwise.

118. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiffs and the Class and the importance of exercising reasonable care in handling it.

119. Defendant breached its duties by failing to exercise reasonable care in supervising its employees, agents, contractors, vendors, and suppliers, and in handling and securing the PII of Plaintiffs and the Class which actually and proximately caused the Data Breach and Plaintiffs' and the Class's injury. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs' and members of the Class's injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiffs and the Class have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

120. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiffs and members of the Class actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiffs and the Class)

121. Plaintiffs reallege all previous paragraphs as if fully set forth below.

122. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and the Class's PII.

123. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers or, in this case, consumers' PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiffs' and the members of the Class's PII.

124. Defendant breached its duties to Plaintiffs and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII.

125. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII.

126. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiffs' and the Class's PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII Defendant collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense

damages that would result to individuals in the event of a breach, which ultimately came to pass.

127. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

128. But for Defendant's wrongful and negligent breach of the duties owed to Plaintiffs and members of the Class, Plaintiffs and members of the Class would not have been injured.

129. The injury and harm suffered by Plaintiffs and members of the Class were the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties and that its breach would cause Plaintiffs and members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

130. Had Plaintiffs and the Class known that Defendant did not adequately protect their PII, Plaintiffs and members of the Class would not have entrusted Defendant with their PII.

131. Defendant's various violations and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

132. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of PII; harm resulting from damaged credit scores and information; and other harm

resulting from the unauthorized use or threat of unauthorized use of stolen PII, entitling them to damages in an amount to be proven at trial.

133. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and Class members have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect their PII in its continued possession.

COUNT III
Breach of Contract
(On Behalf of Plaintiff Whelan and the Class)

134. Plaintiffs reallege all previous paragraphs as if fully set forth below.

135. Defendant entered into various contracts, including consulting companies, to provide its services to its clients.

136. These contracts are virtually identical to each other and were made expressly for the benefit of Plaintiff and the Class, as it was their confidential information that Defendant agreed to collect and protect through its services. Thus, the benefit of collection and protection of the PII belonging to Plaintiff and the Class were the direct and primary objective of the contracting parties.

137. Defendant knew that if it were to breach these contracts with its consulting provider clients, the clients' employees and consumers, including Plaintiff and the Class, would be harmed by, among other things, fraudulent misuse of their PII.

138. Defendant breached its contracts with its clients when it failed to use reasonable data security measures that could have prevented the Data Breach and resulting compromise of Plaintiff's and Class Members' PII.

139. As reasonably foreseeable result of the breach, Plaintiff and the Class were harmed by Defendant failure to use reasonable data security measures to store their PII, including but not limited to, the actual harm through the loss of their PII to cybercriminals.

140. Accordingly, Plaintiff and the Class are entitled to damages in an amount to be determined at trial, along with their costs and attorney fees incurred in this action.

COUNT IV
Breach of Implied Contract
(On Behalf of Plaintiff Emerick, Plaintiff Albert, and the Class)

141. Plaintiffs reallege all previous paragraphs as if fully set forth below.

142. Plaintiffs and Class Members were required to provide their PII Defendant as a condition of applying and receiving employment from Defendant. Plaintiffs and Class Members provided their PII to Defendant in exchange for Defendant's employment and application for employment.

143. Plaintiffs and Class Members reasonably understood that a portion of the funds from their employment would be by Defendant used to pay for adequate cybersecurity and protection of their PII.

144. Plaintiffs and the Class Members accepted Defendant's offers by disclosing their PII to Defendant in exchange for an application for employment and employment.

145. In turn, and through internal policies, Defendant agreed to protect and not disclose the PII to unauthorized persons.

146. In its Privacy Policy, Defendant represented that they had a legal duty to protect Plaintiffs' and Class Member's PII.

147. Implicit in the parties' agreement was that Defendant would provide Plaintiffs and Class Members with prompt and adequate notice of all unauthorized access and/or theft of their PII.

148. After all, Plaintiffs and Class Members would not have entrusted their PII to Defendant in the absence of such an agreement with Defendant.

149. Plaintiffs and the Class fully performed their obligations under the implied contracts with Defendant.

150. The covenant of good faith and fair dealing is an element of every contract. Thus, parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—and not merely the letter—of the bargain. In short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

151. Subterfuge and evasion violate the duty of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or consist of inaction. And fair dealing may require more than honesty.

152. Defendant materially breached the contracts it entered with Plaintiffs and Class Members by:

a. failing to safeguard their information;

b. failing to notify them promptly of the intrusion into its computer systems that compromised such information.

c. failing to comply with industry standards;

d. failing to comply with the legal obligations necessarily incorporated into the agreements; and

e. failing to ensure the confidentiality and integrity of the electronic PII that Defendant created, receive and maintained.

153. In these and other ways, Defendant violated its duty of good faith and fair dealing.

154. Defendant's material breaches were the direct and proximate cause of Plaintiffs' and Class Members' injuries (as detailed *supra*).

155. Plaintiffs and Class Members performed as required under the relevant agreements, or such performance was waived by Defendant's conduct.

COUNT V
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

156. Plaintiffs reallege all previous paragraphs as if fully set forth below.

157. Plaintiffs and members of the Class conferred a benefit upon Defendant in providing PII to Defendant.

158. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiffs and the Class. Defendant also benefited from the receipt of Plaintiffs' and the Class's PII, as this was used to facilitate its services to Plaintiffs and the Class.

159. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' PII.

160. Instead of providing a reasonable level of security, or retention policies, which would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective

security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

161. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiffs' and the Class's PII because Defendant failed to adequately protect their PII.

162. Plaintiffs and Class Members have no adequate remedy at law.

163. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs and members of the Class all unlawful or inequitable proceeds received by them because of their misconduct and Data Breach.

COUNT VI
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and the Class)

164. Plaintiffs reallege all previous paragraphs as if fully set forth below.

165. Given the relationship between Defendant and Plaintiffs and Class Members, where Defendant became guardian of Plaintiffs' and Class Members' PII, Defendant became a fiduciary by its undertaking and guardianship of the PII, to act primarily for Plaintiffs and Class Members, (1) for the safeguarding of Plaintiffs' and Class Members' PII; (2) to timely notify Plaintiffs and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

166. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of Defendant's relationship with them—especially to secure their PII.

167. Because of the highly sensitive nature of the PII, Plaintiffs and Class Members would not have entrusted Defendant, or anyone in Defendant's position, to retain their PII had they known the reality of Defendant's inadequate data security practices.

168. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to sufficiently encrypt or otherwise protect Plaintiffs' and Class Members' PII.

169. Defendant also breached its fiduciary duties to Plaintiffs and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

170. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

COUNT VII
Violation Of The New York Deceptive Trade Practices Act ("GBL")
New York Gen. Bus. Law § 349
(On Behalf of Plaintiffs and the Class)

171. Plaintiffs reallege all previous paragraphs as if fully set forth below.

172. Defendant engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce and furnishing of services, in violation of N.Y. Gen. Bus. Law § 349(a), including but not limited to the following:

a. Misrepresenting material facts to Plaintiffs and the Class by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Class Members' PII from unauthorized disclosure, release, data breaches, and theft;

b. Misrepresenting material facts to Plaintiffs and the Class by representing that they did and would comply with the requirements of federal and state laws pertaining to the privacy and security of Class Members' PII;

c. Omitting, suppressing, and/or concealing material facts of the inadequacy of its privacy and security protections for Class Members' PII;

d. engaging in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Class Members' PII, in violation of duties imposed by and public policies reflected in applicable federal and state laws; and,

e. engaging in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Data Breach to the Class in a timely and accurate manner, contrary to the duties imposed by N.Y. Gen. Bus. Law § 899-aa(2).

173. Defendant knew or should have known that its network and data security practices were inadequate to safeguard the Class Members' PII entrusted to it, and that risk of a data breach or theft was highly likely.

174. Defendant should have disclosed this information because Defendant was in a superior position to know the true facts related to the defective data security.

175. Defendant's failure constitutes false and misleading representations, which have the capacity, tendency, and effect of deceiving or misleading consumers (including Plaintiffs and Class Members) regarding the security of Defendant's network and aggregation of PII.

176. The representations upon which consumers (including Plaintiffs and Class Members) relied were material representations (e.g., as to Defendant's adequate protection of PII), and consumers (including Plaintiffs and Class Members) relied on those representations to their detriment.

177. Defendant's conduct is unconscionable, deceptive, and unfair, as it is likely to, and did, mislead consumers acting reasonably under the circumstances. As a direct and proximate result of Defendant's conduct, Plaintiffs and other Class Members have been harmed, in that they were not timely notified of the Data Breach, which resulted in profound vulnerability to their personal information and other financial accounts.

178. Defendant knew or should have known that their computer systems and data security practices were inadequate to safeguard Class Members' PII and that the risk of a data security incident was high.

179. Defendant's acts, practices, and omissions were done in the course of Defendant's business of furnishing employment benefit services to consumers in the State of New York. 167.

180. As a direct and proximate result of Defendant's unconscionable, unfair, and deceptive acts and omissions, Plaintiffs' and Class Members' PII was disclosed to third parties without authorization, causing and will continue to cause Plaintiffs and Class Members damages.

181. Plaintiffs and Class Members were injured because:

a. Plaintiffs and Class Members would not have accepted employment at Defendant had they known the true nature and character of Defendant's data security practices;

b. Plaintiffs and Class Members would not have entrusted their PII to Defendant in the absence of promises that Defendant would keep their information reasonably secure, and

c. Plaintiffs and Class Members would not have entrusted their PII to Defendant in the absence of the promise to monitor their computer systems and networks to ensure that they adopted reasonable data security measures.

182. Defendant's multiple, separate violations of GBL §349 were the direct and proximate cause of Plaintiffs' and Class Members' injuries (as detailed supra).

183. As a result, Plaintiffs and the Class Members have been damaged in an amount to be proven at trial.

184. Plaintiffs bring this action on behalf of themselves and Class Members for the relief requested above and for the public benefit to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiffs , Class Members and the public from Defendant's unfair, deceptive, and unlawful practices. Defendant's wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

185. Plaintiffs and Class Members seek relief under N.Y. Gen. Bus. Law § 349(h), including, but not limited to, actual damages, treble damages, statutory damages, injunctive relief, and/or attorney's fees and costs.

186. On behalf of themselves and other members of the Class, Plaintiffs seek to enjoin the unlawful acts and practices described herein, to recover their actual damages or fifty dollars, whichever is greater, three times actual damages, and reasonable attorneys' fees.

187. Also as a direct result of Defendant's violation of GBL § 349, Plaintiffs and the Class Members are entitled to damages as well as injunctive relief, including, but not limited to, ordering Defendant to: (i) strengthen their data security systems and monitoring procedures;

(ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

PRAYER FOR RELIEF

Plaintiffs and the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiffs and the proposed Class, appointing Plaintiffs as class representatives, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiffs and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiffs and the Class;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII;

E. Awarding Plaintiffs and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiffs and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiffs and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

Dated: March 25, 2024

Respectfully submitted,

By: /s/ James Bilsborrow___

James Bilsborrow
WEITZ & LUXENBERG, PC
700 Broadway
New York

TURKE & STRAUSS LLP
Samuel J. Strauss
Raina Borrelli
613 Williamson Street, Suite 201
Madison, Wisconsin 53703
Telephone: (608) 237-1775
Facsimile: (608) 509-4423
sam@turkestrauss.com
raina@turkestrauss.com

Attorneys for Plaintiffs and Proposed Class